Identity Landscape: OpenID® for MNOs

Presentation to the GSMA IDG and IDC

Bjorn Hjelm – Vice Chair OIDF

Gail Hodges – Executive Director, OpenID Foundation
Our conversation today... 

- What is the OpenID Foundation
- Current identity trends
- What OIDF Standards can do for MNOs
- Big changes, and big opportunities
What is the OpenID Foundation?

- Non-profit open standards body focused on identity infrastructure enables billions of transactions per day

- Global adoption includes:
  
  - **OpenID Connect** – Verify a user and get basic user profile information to a relying party.
    - Wide application: web & mobile, enterprise & consumer, on prem & cloud, federated vs user, basic claims & multiple claims
    - Android, Apple, AOL, Deutsche Telekom, Google, GSMA Mobile Connect, KDDI, Microsoft, NEC, NTT, Orange, Salesforce, Softbank, Symantec, Telefónica, Verizon, Yahoo! Japan

  - **FAPI** – A security profile for APIs to authenticate the sender, receiver, user, message while retaining confidentiality and averting phishing and replay attacks.
    - Open Banking (UK, Australia, Brazil, US/Canada, Russia)
    - Applicable across verticals, facilitates global interoperation

- Emerging trends are driving new OIDF standards & adoption
Current Identity Trends

- Mobile as enabler
- Vertical convergence (Identity, finance, big tech, MNO, health)
- Convergence of digital & physical identity
- Legislative Action (Privacy, Inclusion, Security)
- Open Banking to Open Data
- Zero Trust + Cloud Architecture
- Passwordless Authentication
What OpenID Standards can do for you

MNO use cases that use OIDF Standards

1. MNO as an Identity Service Provider
2. MNO that wants to Verify Attributes
3. MNOs that want to Share Signals
4. MNO as a Relying Party to Third Party Identity Services
5. MNO that need to Conform to Open Banking (Data) Regulations
6. MNO Identity Services for Employees, Systems, & Things

Each MNO will think strategically whether to engage in (1)-(3), and how they can optimize their investments in (4)-(6)
MNO as an Identity Service Provider

MNO offers user Identity Service (usually $0) and offers identity service to relying parties (usually $).

MNO Best Fit

- Trusted brand
- Pervasive use of services through the MNO (e.g. payment, social media platforms)
- User sees Identity service as a natural extension
- Relying parties see MNO as a natural identity service provider

OIDF Standards

- OpenID Connect + MODRNA
  - Three party model: MNO, User, and Relying party, requires secure and federated exchange of identity data
  - MNO specific requirements addressed in MODRNA spec
  - CIBA protocol allows relying parties to exchange data direct with Identity Service provider without browser redirects
  - Certification available

Live Examples

- ZenKey
  - Verizon, T-Mobile, AT&T joint entity offering identity services to relying parties
  - Case study in OIDF Workshop
MNO that wants to verify attributes

MNO as verifier of user data like mobile number, billing address, name, for a user (usually $0) to a relying party (usually $).

- Financial upside
- Strengthening identity services for ecosystem as a whole

- OpenID Connect for Identity Assurance
  - Three party model: MNO, User, and Relying party, secure and federated exchange of identity data
  - Standard is extensible to a wide range of identity providers (banks, MNOs, mDLs/Digital IDs, verifiable credentials)
  - Standard is extensible to any trust framework, relying party vertical and use case
  - Certification available

- GAIN Whitepaper
  - Success in a few markets, financial service sector “led” models
  - GAIN whitepaper as a vision for this model at global scale, a global assured identity layer for the internet
  - GAIN POC

MNO Best Fit

MNOs that see value in serving wider ecosystem

OIDF Standards

Live Examples

Bank ID, SecureKey, Yes.com
MNOs that want to Share Signals with 3rd Parties

MNO that sees the value in sharing data with trusted 3rd parties to jointly (and collectively) mitigate fraud

MNO Best Fit

- MNOs with sophisticated fraud teams
- MNOs that see the inherent value in sharing data to fight cybercrime
- MNOs with the technical ability to generate and exchange signals with selected partners
- Reduce the cost of ownership for risk data previously only generated and consumed in house (e.g. Sim swap, phone number change)
- Strengthening identity services for ecosystem as a whole

OIDF Standards

- Shared Signals & Events
- Two party: Entity 1 & Entity 2 that mutually agree to share data, using standards that allows interoperability with other parties technically
- Standard is extensible to a wide range of ecosystem participants (e.g. digital platforms, banks, MNOs)

Live Examples

- ZenKey
- SSE WG leads e.g. Google, Amazon, Microsoft
- Success in a few markets, financial service sector “led” models
- GAIN whitepaper as a vision for this model at global scale, a global assured identity layer for the internet
- GAIN POC
MNO as a Relying Party for 3rd Party Identity Services

MNO that wants to improve user experience while simplifying how data is consumed lowering switching costs

### MNO Best Fit
MNOs that invest in test & learn on new UX & technology

- Pilots/ proof of concept to prove out incremental value, e.g. data verified by a bank improves user onboarding process, an mDL on a user device allows for instant account opening.

### OIDF Standards
OpenID Connect for Identity Assurance
Open ID Connect Self-Issued Identity Provider

- Relying party received data in a standardized data structure (not bespoke vendor SDKs)
- Relying party receives data on the Trust Framework used to generate the data, simplifying the RP ability to make decisions on the data received.
- Relying party can consume an mDL/ Digital ID held on the users device

### Live Examples
GAIN POC
mDL

- Gain POC is forming now, with kick off in December, including global participants from financial services, IdPs, leading RPs
- mDLs are gaining traction in some markets (Australia, US, Colombia), using ISO18013-5 standards that are extensible to other credentials, and web/app use cases
MNOs in many markets already expect Open Banking regulation to apply to their industry and expand to Open Data including MNOs.
MNO Identity services for Employees, Systems, Things

MNOs need to identify employees, enable access to internal systems & buildings, access to things (e.g. devices, IoT), and suppliers

- **MNO Best Fit**
  - All
  - Need to identify employees
  - Often legal obligations to identify supplier
  - Work from home/ take your device to work programs distribute devices
  - Staff devices, IoT, fleets of cars-distributed and networked “things”

- **OIDF Standards**
  - Open ID Connect + Profiles
  - Depends on use case

- **Live Examples**
  - Emerging
  - Watch this space!
Big changes, big opportunities

“Vertical convergence” (Identity, finance, big tech, MNO, health)

“Convergence of digital & physical identity”

“Mobile as enabler”

A vision introduced at the European Cloud Identity Conference:

The Global Assured Identity (GAIN) Whitepaper
The GAIN hypothesis for global interoperability

The crowdsourced paper simply suggests a start— and the means to catalyze the global community to action.
Relying Parties (RPs)
- Use ‘IDP Chooser’
- Request and receive verified user claims from the user selected IDP
- Conformance test

Identity Providers (IDPs)
- Connect their own claim sources to OpenID Connect 4 Identity Assurance API
- Deliver verified user claims with the user’s consent to RPs
- Conformance test
<table>
<thead>
<tr>
<th>Time</th>
<th>Session</th>
<th>Speaker(s)</th>
</tr>
</thead>
</table>
| 3:00 to 3:10pm CET | Introduction by Workshop Hosts | Helene Vigue – IDC, GSMA  
Bjorn Helm - Vice-Chair OpenID Foundation  
Gail Hodges - Executive Director, OpenID Foundation |
| 3:10 - 3:40 | ZenKey Case Study: A multifactor authentication service for apps and the web from Verizon, AT&T, T-Mobile using the OpenID Connect & MODRNA standards. | Michael Engan – T-Mobile, USA |
| 3:40-4:00 | Mobile Connect Update: IDG Overview         | Gautam Hazari – IDG, GSMA  
Dawid Wroblewski – Deutsche Telekom, Co-Chair IDG |
| 4:00-4:20 | OpenID Foundation MODRNA standard            | Bjorn Helm - Vice-Chair OpenID Foundation |
| 4:20-4:50 | OpenID Connect for Identity Assurance        | TBC: Co-chair eKYC & IDA WG  
TBC: Co-Chair GAIN POC  
To join POC: GAINPOC@oidf.org |
| 4:50-5:30 | Break                                        |                                                   |
| 5:00-5:10 | OpenID Connect Grant Management              | Co-Chair OIDC WG |
| 5:10-5:30 | Shared Signals & Events                      | TBC: Shared Signals and Events WG Group Co-chair |
| 5:30-5:45 | Open Banking & Open Data and the Financial-Grade API security profile | TBC: FAPI WG Co-Chair |
| 5:45-6:00pm | Questions & Wrap                             | Helene Vigue  
Gautam Hazari  
Bjorn Helm  
Gail Hodges |

**Call to Action:**

- Join the OIDF Workshop Date TBC 11/29 or 11/30
- Join the OIDF as a Member and any WGs of interest at openid.net
- Join the GAIN POC at GAINPOC@oidf.org
Appendix